

Efficient Certificateless Signcryption Tag-KEMs for Resource-constrained Devices

Wenhao Liu¹, Maurizio Adriano Strangio² and Shengbao Wang¹

¹ Hangzhou Normal University,
School of Information Sciences and Engineering, Hangzhou, Zhejiang, China

² University of Rome “Roma Tre”,
Department of Mathematics and Physics, Rome, Italy

Abstract. Efficient certificateless one-pass session key establishment protocols can be constructed from key encapsulation mechanisms (KEMs) by making use of tags and signcryption schemes. The resulting primitives are referred to as Certificateless Signcryption Tag Key Encapsulation Mechanisms (CLSC-TKEMs). In this paper we propose two novel CLSC-TKEM protocols, the first, named LSW-CLSC-TKEM, makes use of the signature scheme of Liu et al., the second, named DKTUTS-CLSC-TKEM, is based on the direct key transport using a timestamp (DKTUTS) protocol first described by Zheng. In order to achieve greater efficiency both schemes are instantiated on elliptic curves without making use of pairings and are therefore good candidates for deployment on resource constrained devices.

1 Introduction

Certificateless cryptography (CLC), introduced by Al-Riyami and Paterson [1], does not require a public-key infrastructure (PKI) for digital certificate management and does not suffer from the inherent key escrow feature of identity-based cryptography (IBC). A certificateless scheme continues to make use of a trusted third party known as the key generating center (KGC) which, as opposed to IBC, does not have access to the user’s private key. In the CLC setting user private keys are constructed from two partial secrets: one generated by the KGC computed from the user’s identity and a secret master key and a secret value chosen by the user itself. The scheme is not identity-based, because the public key is no longer exclusively computable from a user’s identity. When Alice wants to send a message to Bob using a certificateless scheme, she must obtain Bob’s public key. However, no authentication of Bob’s public key is necessary and no certificate is required (as normally would be the case with a PKI).

The generation of a cryptographic secret key and its encryption with a public key encryption scheme is generally known as key encapsulation mechanism (KEM). Further encrypting a message with the secret key and a symmetric key encryption scheme is known as a data encryption mechanism (DEM). In general, the resulting KEM-DEM schemes combine advantages of both symmetric and asymmetric cryptographic techniques thus giving rise to secure and efficient hybrid public key encryption schemes [2,3]. Efficient one-pass session key establishment protocols [4] can be constructed based on KEMs by making use of tags [5] and signcryption schemes [6] appropriately

instantiated in the CLC setting. The resulting primitives are referred to as Certificateless Signcryption Tag Key Encapsulation Mechanisms (CLSC-TKEMs). The use of a signcryption scheme implies additional important security properties such as user (sender) non-repudiation which are derived from the use of a digital signature scheme.

In this paper we propose two CLSC-TKEM protocols, the first, named LSW-CLSC-TKEM, makes use of the signature scheme of Liu et al. [7], the second, named DKTUTS-CLSC-TKEM, is based on the direct key transport using a timestamp (DKTUTS) protocol described in [8]. In order to achieve greater efficiency both schemes can be instantiated on elliptic curves without making use of pairings and are therefore ideal candidates for deployment on resource constrained devices.

2 Related work

In recent work, Jongho Won *et al.* [9] proposed an efficient CLSC-TKEM protocol (eCLSC-TKEM) for securing communications between drones and smart objects. According to the authors, the protocol supports authenticated key agreement, non-repudiation, and user revocation and significantly reduces the time required to establish a shared key between a drone and a smart object by minimizing the computational overhead on the smart object (since the protocol does not make use of pairings). A problem with this protocol is possibly due to the user revocation technique introduced by the authors which allows expiration of user partial private keys and therefore requires subsequent reissue of a key and distribution to the user by the KGC. Much like the aforementioned protocol, the CLSC-TKEM scheme of Seo *et al.* [10] is also inefficient from the computational perspective if the target recipient is a low-power resource-limited device.

In [11] the authors propose a generic architecture for a CLSC-TKEM that is based on a true random number generator (TRNG) to produce secure cryptographic secret keys for a KEM/DEM scheme.

3 Theoretical Framework for Certificateless Signcryption Tag-KEMs

We refer to the framework of Signcryption Tag-KEMs (SC-TKEM) introduced by Bjorstad and Dent [12] and extend it to the CLC setting. A CLSC-TKEM is defined as the tuple of six algorithms described below:

1. **Setup:** A probabilistic common parameter generation algorithm that takes as input a security parameter 1^k and returns all the global system parameters Ω needed by users of the scheme, such as choice of groups or hash functions. The algorithm also outputs the private/public key pair (sk_{KGC}, pk_{KGC}) of the KGC.
2. **PartialPrivateKeyExtract:** A probabilistic key generation algorithm that takes as input the identity ID_E of a generic entity E , Ω and outputs the partial private key d_E of E . This algorithm is generally run by the KGC which must thereafter deliver the partial private key d_E to E through a secure channel.
3. **GenUserKeys:** A probabilistic key generation algorithm that takes as input Ω and generates the private/public key pair (x_E, P_E) of entity E . Entity E sets $sk_E = (x_E, d_E)$ as its full private key.

4. **SymmetricKeyGen:** A probabilistic symmetric key generation algorithm that takes as input the public key pk_B of the recipient entity B and outputs the symmetric key K and internal state information ω .
5. **Encapsulation:** A probabilistic key encapsulation algorithm that receives as input the state information ω , an arbitrary tag τ , the full private key sk_A of the sender A and returns an encapsulation ϕ .
6. **Decapsulation:** A deterministic decapsulation/verification algorithm that takes as input the public key pk_A of the sender A , the full private key sk_B of the recipient, an encapsulation ϕ and a tag τ and returns either the symmetric key K or the unique error symbol \perp .
For the CLSC-TKEM to be sound, the decapsulation/verification algorithm must return the correct key K whenever the encapsulation ϕ is correctly formed and the corresponding keys and tag are supplied.

4 The LSW-CLSC-TKEM protocol specification

The LSW-CLSC-TKEM protocol, based on the signature scheme of Liu et al. [7], is completely specified by the six polynomial time algorithms specified below:

1. **Setup:** On input the security parameter $k \in \mathbb{Z}^+$, the KGC returns the system parameters Ω (see below) and the KGC's master private key x_{msk} . The KGC also performs the following steps:
 - Chooses a k -bit prime q , generates a cyclic additive group G , a cyclic multiplicative group G_2 both of order q and defines the tuple $\langle F_q, E/F_q, G, G_2, P \rangle$, with P generator of G .
 - Chooses the master key $x_{msk} \in_R \mathbb{Z}_q^*$ uniformly at random and computes the system public key $P_{pub} = x_{msk}P$.
 - Chooses the cryptographic hash functions $H_1 : \{0, 1\}^* \times G \rightarrow \mathbb{Z}_q^*$, $H_2 : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$ and $H_3 : \{0, 1\}^* \rightarrow \{0, 1\}^*$;
 - Publishes the global system parameters $\Omega = \langle F_q, E/F_q, G, G_2, P, P_{pub}, H_1, H_2 \rangle$.
2. **PartialPrivateKeyExtract:** For entity A , with identity ID_A , the KGC chooses $r_A \in_R \mathbb{Z}_q^*$ computes $R_A = r_AP$, $h_A = H_1(ID_A, R_A)$, $d_A = r_A + x_{msk}h_A \bmod q$ and delivers the partial private key d_A to user ID_A through a secret channel. Entity A can validate her key by verifying that $d_AP = R_A + h_AP_{pub}$.
3. **GenUserKeys:** Entity A with an identity ID_A chooses $x_A \in_R \mathbb{Z}_q^*$ as its secret value and generates the corresponding public key $P_A = x_AP$. Furthermore, entity A sets $sk_A = (x_A, d_A)$ as its full private key and $pk_A = (P_A, R_A)$ as its full public key.
4. **SymmetricKeyGen:** Given the sender identity ID_A , the receiver identity ID_B and the full public key pk_B as inputs, entity A (the sender) proceeds as follows:
 - Chooses $u_A \in_R \mathbb{Z}_q^*$ and computes $U = u_A(R_B + H_1(ID_B, R_B)P_{pub} + P_B)$;
 - Computes $X = u_AP$ and $K = H_1(X, U, ID_A, ID_B)$;
 - Outputs K and $\omega = (u_A, ID_A, sk_A, ID_B, pk_B, X, U)$.
5. **Encapsulation:** On input ω , an arbitrary tag τ , the full private key sk_A , entity A obtains the encapsulation ϕ by performing the following operations:
 - Selects $a \in_R \mathbb{Z}_q^*$ and computes $Q = aP$;

- Computes $h = H_2(\tau, ID_A, ID_B, R_A, R_B, P_A, P_B, Q, X, U)$;
 - Computes $s = a/(hx_A + d_A)$;
 - Sets $\sigma = (s, h)$ and outputs $\phi = \langle Q, U, \sigma \rangle$.
6. **Decapsulation:** On input the encapsulation ϕ , tag τ , the sender's identity ID_A , full public key pk_A , the receiver's identity ID_B and the full private key sk_B , the recipient entity B performs the following operations:
- Computes $(d_B + x_B)^{-1} \cdot U = u_A P = X$;
 - Computes $h = H_2(\tau, ID_A, ID_B, R_A, R_B, P_A, P_B, Q, X, U)$;
 - If $s(hP_A + R_A + H_1(ID_A, R_A)P_{pub}) \neq Q$, returns with an invalid encapsulation error \perp ;
 - Otherwise, accepts the key $K = H_1(X, U, ID_A, ID_B)$.

The correctness of the protocol is determined as follows:

$$\begin{aligned}
s(hP_A + R_A + H_1(ID_A, R_A)P_{pub}) &= a(hx_A + d_A)^{-1}(hP_A + R_A + h_AP_{pub}) \\
&= a(hx_A + d_A)^{-1}(hx_AP + r_AP + h_AxP) \\
&= a(hx_A + d_A)^{-1}(hx_A + r_A + h_Ax)P \\
&= a(hx_A + d_A)^{-1}(hx_A + d_A)P \\
&= aP = Q
\end{aligned}$$

5 The DKTUTS-CLSC-TKEM protocol specification

The DKTUTS-CLSC-TKEM protocol, based on the direct key transport using a timestamp (DKTUTS) protocol described in [8], is completely specified by the six polynomial time algorithms specified below:

1. **Setup:** On input the security parameter $k \in \mathbb{Z}^+$, the KGC returns two system parameters: Ω and the KGC's master private key x_{msk} . The KGC also performs the following steps:
 - Chooses a k -bit prime q , generates a cyclic additive group G , a cyclic multiplicative group G_2 both of order q and determines the tuple $\langle F_q, E/F_q, G, G_2, P \rangle$, with P generator of G .
 - Chooses the master key $x_{msk} \in_R \mathbb{Z}_q^*$ uniformly at random and computes the system public key $P_{pub} = x_{msk}P$.
 - Chooses the cryptographic hash functions $H_1 : \{0, 1\}^* \times G \rightarrow \mathbb{Z}_q^*$, $H_2 : \mathbb{Z}_q^* \rightarrow \{0, 1\}^*$ and a keyed hash function $F_K : \{0, 1\}^* \rightarrow \{0, 1\}^*$;
 - Chooses the symmetric encryption scheme $(E_K(\cdot), D_K(\cdot))$;
 - Publishes the global system parameters $\Omega = \langle F_q, E/F_q, G, G_2, P, P_{pub}, H_1, H_2, KH, E, D \rangle$.
2. **PartialPrivateKeyExtract:** For entity A , with identity ID_A , the KGC chooses $r_A \in_R \mathbb{Z}_q^*$ computes $R_A = r_AP$, $h_A = H_1(ID_A, R_A)$, $d_A = r_A + x_{msk}h_A \bmod q$ and delivers the partial private key d_A to user ID_A through a secret channel. Entity A can validate her key by verifying that $d_AP = R_A + h_AP_{pub}$.
3. **GenUserKeys:** Entity A with an identity ID_A chooses $x_A \in_R \mathbb{Z}_q^*$ as its secret value and generates the corresponding public key as $P_A = x_AP$. Furthermore, entity A sets $sk_A = (x_A, d_A)$ as its full private key and $pk_A = (P_A, R_A)$ as its full public key.

4. **SymmetricKeyGen:** Given the sender identity ID_A , the receiver identity ID_B and the full public key pk_B as input, the sender proceeds as follows:
 - Chooses $K \in_R \{0, 1\}^{l_k}$ and $x, a \in_R \mathbb{Z}_q^*$;
 - Computes $U = aP$ and $X = x(R_B + H_1(ID_B, R_B)P_{pub} + P_B)$;
 - Computes $(k_1, k_2) = H_2(X + U)$;
 - Outputs K and $\omega = (x, k_1, k_2, TS, ID_A, ID_B, pk_B, X, U)$ where TS is a suitably defined timestamp.
5. **Encapsulation:** On input ω , an arbitrary tag τ , the full private key sk_A , entity A obtains the encapsulation ϕ by performing the following computations:
 - Computes $c = E_{k_1}(K, TS, \tau, ID_A, ID_B, R_A, R_B, P_A, P_B, X, U)$,
 $r = F_{k_2}(K, TS, \tau, ID_A, ID_B, R_A, R_B, P_A, P_B, X, U)$
 and $s = x/(r + x_A) \bmod q$;
 - Outputs $\phi = \langle U, c, r, s \rangle$.
6. **Decapsulation:** On input the encapsulation ϕ , tag τ , the sender's identity ID_A , full public key pk_A , the receiver's identity ID_B and the full private key sk_B , the recipient entity B performs the following computations:
 - Computes $X' = s(d_B + x_B)(P_A + rP)$ and $H_2(X' + U) = (k_1, k_2)$;
 - Computes $K, TS, \tau, ID_A, ID_B, R_A, R_B, P_A, P_B, X, U' = D_{k_1}(c)$ and
 $r' = F_{k_2}(K, TS, \tau, ID_A, ID_B, R_A, R_B, P_A, P_B, X, U')$;
 - If TS is not fresh or $U \neq U'$ or $X' \neq X$ or $r' \neq r$, returns with an invalid encapsulation error \perp ;
 - Otherwise, accepts the key K .

The correctness of the protocol is determined as follows:

$$\begin{aligned}
 s(d_B + x_B)(P_A + rP) &= sd_B(P_A + rP) + sx_B(P_A + rP) \\
 &= s(x_A d_B P + r d_B P) + s(x_A x_B P + r x_B P) \\
 &= s(x_A + r)d_B P + s(x_A + r)P_B \\
 &= x d_B P + x P_B \\
 &= x(d_B P + P_B) = X
 \end{aligned}$$

6 On the efficiency and security of CLSC-TKEM protocols

In this section we compare four CLSC-TKEM protocols from two perspectives: computational load and security properties. Tables 1 and 2 summarize the computational cost of the sender and recipient principals respectively. The features that are taken into account are: a) online and offline exponentiations, the former refer to the operations that are performed during running instances of the protocols while the later consider the pre-computation of values that can be performed before protocol execution (this data must be safely stored in the sender device); b) field inversions (fld inv.); c) field multiplications (fld mult.) and d) decryption operations with a symmetric cipher.

Table 3 summarizes the security properties of the same CLSC-TKEM protocols considered above. The security properties that are taken into account are: a) sender partial forward secrecy (SPFS); b) user authentication (sender); c) non repudiation (sender);

Table 1. Computational efficiency of CLSC-TKEM protocols - sender

<i>Protocol</i>	<i>online exp.</i>	<i>offline exp.</i>	<i>fld inv.</i>	<i>fld mult.</i>	<i>encryption</i>
CLSC-TKEM[10]	2EM	0EM	0	2	0
eCLSC-TKEM[9]	4EM	2EM	0	0	0
LSW-CLSC-TKEM	3EM	0EM	1	2	0
DKTUTS-CLSC-TKEM	2EM	0EM	1	1	1

Table 2. Computational efficiency of CLSC-TKEM protocols - recipient

<i>Protocol</i>	<i>online exp.</i>	<i>offline exp.</i>	<i>fld inv.</i>	<i>fld mult.</i>	<i>decryption</i>
CLSC-TKEM[10]	5EM	3EM	0	0	0
eCLSC-TKEM[9]	4EM	2EM	0	0	0
LSW-CLSC-TKEM	3EM	0EM	1	0	0
DKTUTS-CLSC-TKEM	2EM	0EM	0	1	1

d) user revocation; e) security proof, indicates whether a formal security proof exists for the protocol.

All protocols considered in table 3 do not guarantee *forward secrecy* (FS). For these typical one-pass key transport schemes where the recipient does not contribute to the computation of the session key the appropriate notion is that of *partial forward secrecy* (PFS) i.e. if compromise of the long-term keys of one or more specific principals does not compromise the session keys established in previous protocol runs involving those principals [13]. In particular, for the protocols we are discussing it makes sense to consider *sender partial forward secrecy* [4] (respect to a passive adversary that can corrupt peers to obtain long-term keying material such as the private key and that does not modify protocol messages in transit through the network).

Table 3. Security properties of CLSC-TKEM protocols

<i>Protocol</i>	<i>sPFS</i>	<i>user auth.</i>	<i>non-repud.</i>	<i>user revoc.</i>	<i>sec. proof</i>
CLSC-TKEM[10]	yes	yes	yes	no	yes
eCLSC-TKEM[9]	yes	yes	yes	yes	yes
LSW-CLSC-TKEM	yes	yes	yes	no	no
DKTUTS-CLSC-TKEM	yes	yes	yes	no	no

7 Final remarks

In this paper we have addressed the problem, introduced by [9], of ensuring that drones can perform secure communications with many different smart objects, such as sensors and embedded devices. The authors propose a Certificateless Signcryption Tag Key Encapsulation Mechanism (eCLSC-TKEM) that minimizes the computational load on the receiving resource-constrained mobile device. We have proposed two constructions

that achieve better performance in terms of the computational overhead required by the recipient.

However, resource-constrained devices are often more susceptible to private key exposure therefore forward secrecy (of the recipient) may be indeed a desirable security property for the above protocols. Depending on the target application, when forward secrecy is necessary a possible option is to employ two-pass key agreement protocols at the expense of a greater computational cost for the recipient (the protocols described in this paper can be modified into equivalent key agreement versions). Another possibility of mitigating the consequences of user corruption by an adversary is to use a key evolving mechanism so that keys are updated periodically and thus damage is limited to the period of validity of the exposed key [14].

References

1. S.S. Al-Riyami and K.G. Paterson *Certificateless public key cryptography* Advances in Cryptology- ASIACRYPT 2003, LNCS 2894, pp. 452-474, Springer-Verlag, 2003
2. J. Herranz, D. Hofheinz, E. Kiltz *KEM/DEM: Necessary and Sufficient Conditions for Secure Hybrid Encryption* Cryptology ePrint Archive, Report 2006/265, <https://eprint.iacr.org/2006/265.pdf>, 2006
3. A. W. Dent *A Designer's Guide to KEMS* Cryptology ePrint Archive, Report 2002/174, <https://eprint.iacr.org/2002/174.pdf>, 2002
4. M.C. Gorantla, C. Boyd and J.M. Gonzalez Neto *On the Connection between Signcryption and One-pass Key Establishment*, IMA Conference on Cryptography and Coding, 2007
5. M. Abe, R. Gennaro, K. Kurosawa and V. Shoup, *Tag-KEM/DEM: A New Framework for Hybrid Encryption and New Analysis of Kurosawa-Desmedt KEM*, EUROCRYPT 2005, LNCS 3494, pp. 128-146, 2005
6. Y. Zheng, *Digital signcryption or how to achieve Cost (Signature & Encryption) \ll Cost (Signature) + Cost (Encryption)*, Advances in Cryptology, CRYPTO'97, LNCS 1294, pp. 165-179, Springer-Verlag, 1997
7. W. Liu, Q. Xie, S. Wang, L. Han, and B. Hu *Pairing-Free Certificateless Signature with Security Proof*, Hindawi Publishing Corporation, Journal of Computer Networks and Communications Volume 2014, Article ID 792063, 2014
8. Y. Zheng, *Shortened Digital Signature, Signcryption and Compact and Unforgeable Key Agreement Schemes*, Tech. Report, <http://grouper.ieee.org/groups/1363/StudyGroup/Hybrid.html>, A submission to IEEE P1363 Standard Specifications for Public Key Cryptography, 1998
9. Jongho Won and Seung-Hyun Seo and Elisa Bertino, *A Secure Communication Protocol for Drones and Smart Objects*, Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (ASIA CCS '15), pp. 249-260, 2015
10. S. Seo and E. Bertino, *Elliptic curve cryptography based certificateless hybrid signcryption scheme without pairing*, http://www.cerias.purdue.edu/apps/reports_and_papers/view/4698. CERIAS report, 2013
11. I. Thangathiruppathi, S.M. Udhaya Sankar *TRNG Based Key Generation for Certificateless Signcryption* International Conference on Computer Engineering and Information Technology, 2015
12. T. E. Bjrøstsd and W. Dent *Building better Signcryption Schemes with Tag-KEMs* Cryptology ePrint Archive, Report 2005/405, <https://eprint.iacr.org/2005/405.pdf>, 2005
13. C. Boyd and A. Mathuria *Protocols for Authentication and Key Establishment*, Springer-Verlag, 2003

14. M. Franklin *A Survey of Key Evolving Cryptosystems* Int. J. Security and Networks, Vol. 1, Nos. 1/2, 2006
15. M. Abe, R. Gennaro, and K. Kurosawa. *Tag-KEM/DEM: a new framework for hybrid encryption* Journal of Cryptology, Vol. 21, No. 1, pp. 97130, 2008.
16. F. Li, M. Shirase, T. Takagi *Certificateless Hybrid Signcryption* The 5th Information Security Practice and Experience Conference (ISPEC 2009), LNCS 5451, pp. 112123, Springer-Verlag, 2009.